Diogelu data

Canllaw ymarferol i ddiogelwch TG

Delfrydol i fusnes bach



Dywed y Ddeddf Diogelu Data y dylid "dilyn mesurau technegol a sefydliadol priodol yn erbyn proses heb awdurdod neu anghyfreithiol o ddata personol yn erbyn colli damweiniol neu ddinistrio, neu ddifrodi, data personol". Gelwir hyn y seithfed egwyddor diogelu data ac fe'i hesbonnir yn fanylach ar ein gwefan, www.ico.org.uk.

Gall cadw eich systemau TG yn ddiogel fod yn dasg gymhleth ac mae'n galw am amser, adnoddau a gwybodaeth arbenigol. Os oes gennych ddata personol yn eich system TG, mae angen i chi gydnabod y gallai fod dan risg a dilyn mesurau technegol priodol i'w ddiogelu. Dylai'r mesurau a sefydlwch fod yn addas i anghenion eich busnes penodol. Nid oes rhaid iddynt o reidrwydd fod yn ddrud neu'n llafurus. Efallai y byddant hyd yn oed am ddim neu eisoes ar gael yn y systemau TG sydd gennych yn barod.

Rydym wedi cynhyrchu'r canllaw hwn i roi cyngor ymarferol i fusnesau bychain ym maes diogelwch TG.

Beth yw'r fantais i chi?



Gallai mynd yn groes i ddeddfwriaeth diogelu data arwain at godi dirwy ar eich busnes – hyd at £500,000 mewn achosion difrifol. Gallai enw da eich busnes hefyd fod yn y fantol os yw diogelwch annigonol yn cyfrannu at achosion amlwg o golli neu dwyn data.

Fodd bynnag, mae yna fesurau y gallwch eu rhoi ar waith i atal toriadau diogelwch neu gyfyngu'r difrod os byddant yn digwydd.

Y cam cyntaf: asesu'r risg i'ch busnes

Cyn y gallwch sefydlu pa lefel o ddiogelwch sy'n addas i'ch busnes, bydd angen i chi adolygu'r data personol a gedwir gennych ac asesu'r risgiau i'r data hwnnw. Dylech ystyried pob proses wrth i chi gasglu, storio, defnyddio a gwaredu ar ddata personol.

Ystyriwch pa mor werthfawr, sensitif neu gyfrinachol yw'r wybodaeth a pha ddifrod neu drallod a ellid ei achosi i unigolion pe byddai yna doriad diogelwch.

Gyda syniad clir o'r risgiau, gallwch ddechrau dewis y mesurau diogelwch sy'n briodol i'ch anghenion. Y cam nesaf yw dechrau eu rhoi ar waith.

Dilynwch ymagwedd haenog i ddiogelwch

Nid oes un cynnyrch unigol a fydd yn rhoi gwarant 100% i chi o ddiogelwch ar gyfer eich busnes. Yr allwedd i ddiogelwch effeithiol yw dilyn ymagwedd haenog, gan gyfuno nifer o wahanol arfau a thechnegau. Pe byddai un haen yn methu, yna mae eraill ar waith i ddal y bygythiad.

Rhestr Wirio: Defnyddiwch ymagwedd haenog i ddiogelwch

☐ **Diogelwch corfforol**

Mae'n bosib y byddai offer yn cynnwys data personol yn cael ei ddwyn mewn lladrad. Dylech sicrhau bod data personol ar eich systemau wedi ei ddiogelu yn erbyn y bygythiadau hyn. Dylai eich gweinyddwyr fod mewn ystafell ar wahân gyda diogelwch ychwanegol. Ni ddylid gadael dyfeisiadau wrth gefn yn ddioruchwyliaeth a dylid eu cloi ymaith pan nad ydynt mewn defnydd.

☐ **Meddalwedd gwrthfeirysau a gwrthfeddalwedd faleisus**

Dylai fod gennych gynnyrch gwrthfeirysau a gwrthfeddalwedd faleisus yn sganio eich rhwydwaith yn rheolaidd i atal neu ganfod bygythiadau. Byddwch hefyd angen sicrhau eu bod yn gyfredol.

☐ **Amddiffyniad rhag ymyrraeth**

Mae angen i chi allu atal toriadau rhag digwydd cyn iddynt dreiddio'n ddwfn i mewn i'ch rhwydwaith, er enghraifft, trwy ddefnyddio llen dân wedi ei ffurfweddu'n dda.

☐ **Rheoliadau mynediad**

Cyfyngwch fynediad at eich system i ddefnyddwyr a ffynonellau yr ydych yn ymddiried ynddynt. Rhaid i bob defnyddiwr gael ei enw defnyddiwr a chyfrinair ei hun.

Mae ymosodiad cyfrinair grym sylweddol yn ddull cyffredin o ymosodiad, o bosibl hyd yn oed gan ddefnyddwyr achlysurol yn ceisio cael mynediad at eich Wi-Fi felly mae angen i chi orfodi cyfrineiriau cryf, cyfyngu'r nifer o geisiadau aflwyddiannus i fewngofnodi a gorfodi newid cyfrineiriau yn rheolaidd.

Dylid canslo cyfrineiriau neu fynediad arall ar unwaith os bydd aelod o staff yn gadael y sefydliad neu'n absennol am gyfnodau hir.

☐ **Ymwybyddiaeth a hyfforddiant i gyflogeion**

Mae angen i gyflogeion ar bob lefel fod yn ymwybodol o beth yw eu rolau a chyfrifoldebau.

Hyfforddwch eich staff i adnabod bygythiadau megis negeseuon e-bost gwe-rwydo a meddalwedd maleisus arall.

☐ **Segmentiad**

Gallwch atal neu gyfyngu difrifoldeb toriadau data trwy rannu a chyfyngu mynediad rhwng cydrannau eich rhwydwaith. Er enghraifft, dylai eich gweinydd y we fod ar wahân i'ch prif weinydd ffeiliau. Golyga hyn os yw'ch gwefan dan fygythiad ni fyddai gan yr ymosodwr fynediad uniongyrchol at eich storfa data canolog.

☐ **Polisïau**

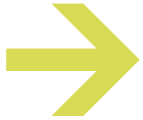
Bydd polisi yn eich galluogi i sicrhau eich bod yn delio â'r risgiau mewn modd cyson. Dylai polisïau sydd wedi eu hysgrifennu'n dda integreiddio'n dda â phrosesau busnes.

☐ **Caledu dyfais**

Dylid cael gwared ar unrhyw feddalwedd a gwasanaethau na ddefnyddir o'ch dyfeisiadau. Mae gan fersiynau hŷn o rai mathau cyffredin o feddalwedd hanes o fod yn agored i ymosodiadau. Os nad ydych yn ei ddefnyddio, yna mae'n llawer haws cael gwared arno na cheisio ei gadw yn gyfredol.

Sicrhewch eich bod wedi newid unrhyw gyfrineiriau diofyn a ddefnyddir gan y meddalwedd neu galedwedd – mae'r rhain yn gyfarwydd i ymosodwyr.





Diogelwch eich data wrth deithio

Beth yw'r broblem?

Mae angen i chi sicrhau y gweithredir yr un lefel o ddiogelwch o ran data personol ar ddyfeisiadau a ddefnyddir tu allan i'r swyddfa. Mae nifer o doriadau data yn deillio o ddwyn neu golli dyfais (e.e. gliniadur, ffôn symudol neu yriant USB), ond dylech hefyd ystyried y diogelwch a ddarperir ar gyfer data y byddwch yn anfon trwy e-bost neu'r post. Gallwch gymryd camau i leihau effeithiau lladrad trwy sicrhau naill ai nad yw'r data personol ar y ddyfais yn y lle cyntaf neu ei fod wedi ei ddiogelu'n briodol fel na ellir cael mynediad ato.

Beth allaf i wneud?

- Mae amgryptiad yn fodd o sicrhau mai dim ond defnyddwyr ag awdurdod sy'n gallu cael mynediad i ddata. Fel arfer, mae angen cyfrinair i 'ddatgloi' y data. Mae rhagor o wybodaeth ar ein gwefan, www.ico.org.uk.
  - Golyga amgryptiad disg llawn fod yr holl ddata ar y cyfrifiadur wedi ei amgryptio.
  - Mae amgryptio ffeil yn golygu y gellir amgryptio ffeiliau unigol.
  - Dylai eich cyfrinair amgryptiad fod yn gymysgedd o lythrennau mawr a bach, rhifau a nodau arbennig (h.y. #, &, !) a dylai fod yn gyfrinachol.
  - Mae rhai meddalwedd yn cynnig amddiffyniad cyfrinair i atal pobl rhag gwneud newidiadau i'r data ond efallai na fydd hyn yn stopio lleidr rhag darllen y data. Sicrhewch eich bod yn gwybod yn union pa lefel o amddiffyniad ydych chi'n defnyddio ar gyfer eich data.
- Mae rhai dyfeisiadau symudol yn cefnogi cyfleuster analluogi neu lanhau o bell. Mae hyn yn eich galluogi i anfon signal i ddyfais a gollwyd neu sydd wedi ei dwyn i'w leoli ac, os oes angen, i ddileu'r holl ddata yn ddiogel.
  - Bydd angen cofrestru eich dyfeisiadau o flaen llaw gyda gwasanaeth fel hyn.
- Dim ond os oes wir ei angen y dylid trosglwyddo data personol i ddyfeisiadau symudol a dylid cael gwared arno unwaith na fydd ei angen.

Eich cadw chi a'ch systemau yn gyfredol

Beth yw'r broblem?

Mae offer a meddalwedd cyfrifiadurol angen gwaith cynnal a chadw rheolaidd i'w gadw'n rhedeg yn esmwyth ac i drwsio unrhyw wendidau diogelwch. Mae meddalwedd diogelwch fel gwrthfeirysau a gwrthfeddalwedd faleisus angen ei ddiweddaru'n rheolaidd i barhau i ddarparu amddiffyniad digonol.

Beth allaf i wneud?

- Sicrhewch fod unrhyw feddalwedd diogelwch sydd gennych wedi ei droi ymlaen ac yn monitro'r ffeiliau fel y dylai.
- Cadwch eich meddalwedd yn gyfredol trwy wirio yn rheolaidd am ddiweddariadau a'u rhoi ar waith. Gellir gosod y rhan fwyaf o feddalwedd i ddiweddaru'n awtomatig.
- Os yw'ch system yn gymharol hen, dylech adolygu'r amddiffyniad sydd gennych i sicrhau ei fod yn dal yn ddigonol.
- Dylech hefyd gadw eich gwybodaeth o fygythiadau yn gyfredol trwy ddarllen bwletinau diogelwch neu gylchlythyrau gan sefydliadau perthnasol i'ch busnes.
- Dylech hefyd roi gwybod i'ch staff am fygythiadau posibl i'ch sefydliad. Gallai hyn gynnwys hysbysu cyflogeion o'r risgiau sy'n gysylltiedig â chyhoeddi gwybodaeth yn ymwneud â'ch gweithgareddau busnes ar rwydweithiau cymdeithasol neu sicrhau eu bod yn gwybod sut i adnabod negeseuon e-bost gwe-rwydo.

Cadw llygad am broblemau

Beth yw'r broblem?

Gall troseddwyr seiber neu feddalwedd faleisus ymosod ar eich systemau heb i neb sylwi am amser hir. Dim ond pan fydd yn rhy hwyr fydd nifer o bobl yn canfod eu bod wedi eu hymosod er bod arwyddion rhybudd yno.



Beth allaf i wneud?

- Gwiriwch eich negeseuon meddalwedd diogelwch, logiau rheoli mynediad a systemau adrodd eraill sydd gennych yn rheolaidd.
- Sicrhewch y gallwch wirio pa feddalwedd neu wasanaethau sy'n rhedeg ar eich rhwydwaith. Sicrhewch y gallwch nodi a oes yn rhywbeth yno na ddylai fod.
- Dylech redeg sganiau gwendid a phrofion treiddiad rheolaidd i sganio'ch systemau ar gyfer gwendidau hysbys – sicrhewch eich bod yn delio ag unrhyw wendidau a nodwyd.



A wyddoch chi beth ddylech fod yn wneud?

Beth yw'r broblem?

Nid oes gan rai sefydliadau lefelau digonol o amddiffyniad am nad ydynt yn defnyddio'r diogelwch sydd ganddynt eisoes yn gywir, ac nid yw'n bosibl gweld pan fydd problem pob tro. Mae angen i chi sicrhau bod eich cyflogeion i gyd yn ymwybodol o'u rolau a chyfrifoldebau a'u bod yn gwybod pan fydd angen gweithredu. Dylech hefyd ystyried pa weithredoedd ddylech eu rhoi ar waith os byddwch yn dioddef toriad data.

Beth allaf i wneud?

- Cymerwch amser i adolygu pa ddata personol sydd gennych ar hyn o bryd a'r dulliau amddiffyn sydd gennych ar waith.
- Sicrhewch eich bod yn cydymffurfio ag unrhyw ganllaw gan y diwydiant neu ofynion cyfreithiol.
- Cofnodwch y rheoliadau sydd gennych ar waith a nodi lle mae angen i chi wneud gwelliannau.
- Unwaith y bydd y gwelliannau wedi eu gweithredu, dylech barhau i fonitro'r rheoliadau a gwneud addasiadau ble fo angen.

- Ystyriwch y risgiau ar gyfer pob math o ddata personol sydd gennych a sut fyddech yn rheoli toriad data. Fel hyn gallwch leihau'r effaith os bydd y gwaethaf yn digwydd.
- Dylech hefyd gael polisi defnydd derbyniol a deunydd hyfforddi i staff fel eu bod yn gwybod beth yw eu cyfrifoldebau diogelu data.
- Gofynnwch i arbenigwr diogelwch adolygu eich systemau. Bydd hyn yn amlygu ble mae eich gwendidau diogelwch a sut i ddelio â nhw.
- Peidiwch ag anghofio i greu copi wrth gefn o'ch data. Dylid creu copïau wrth gefn yn rheolaidd, eu cadw'n ddiogel a'u dileu'n briodol pan nad oes eu hangen mwyach.

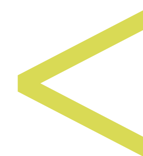
Lleihau eich data

Beth yw'r broblem?

Dywed y Ddeddf Diogelu Data y dylai data personol fod yn gywir, yn gyfredol a'i gadw am ddim mwy nag sydd angen. Gydag amser efallai y byddwch wedi casglu symiau enfawr o ddata personol. Efallai y bydd rhywfaint o'r data hwn wedi dyddio ac yn anghywir neu ddim yn ddefnyddiol bellach.

Beth allaf i wneud?

- Penderfynwch a ydych yn dal angen y data. Os felly, a yw wedi ei storio yn y man cywir?
  - Os oes gennych ddata y mae angen i chi ei gadw at ddibenion archifo, ond nad ydych angen mynediad rheolaidd ato, dylid ei symud i leoliad mwy diogel. Bydd hyn yn helpu atal mynediad heb awdurdod.
- Os oes gennych ddata nad ydych ei angen bellach mewn gwirionedd, dylid ei ddileu. Dylai hyn fod yn unol â'ch polisïau dargadw a gwaredu ar ddata. Efallai y byddwch angen meddalwedd neu gymorth arbenigol i wneud hyn yn ddiogel.



Sicrhewch fod eich contractwr TG yn gwneud beth y dylai fod yn wneud

Beth yw'r broblem?

Mae nifer o fusnesau bychain yn rhoi eu gofynion TG ar gontract allanol i drydydd parti. Dylech fod yn fodlon eu bod yn trin eich data gydag o leiaf yr un lefel o ddiogelwch ag y byddech chi.

Beth allaf i wneud?

- Gofynnwch am archwiliad diogelwch o'r systemau yn cynnwys eich data. Gallai hyn helpu nodi unrhyw wendidau er mwyn i chi fynd i'r afael â nhw.
- Adolygwch gopïau o asesiadau diogelwch eich darparwr TG.
- Os yn briodol, dylid ymweld â swyddfeydd eich darparwr TG i sicrhau eu bod fel y byddech yn disgwyl.
- Gwiriwch y contractau sydd gennych. Rhaid iddynt fod yn ysgrifenedig ac yn gofyn i'ch contractwr weithredu yn unol â'ch cyfarwyddiadau yn unig a chydymffurfio gyda gofynion penodol y Ddeddf Diogelu Data.
- Peidiwch ag esgeuluso gwaredu asedau – os byddwch yn defnyddio contractwr i ddileu data a gwaredu ar neu ailgylchu eich offer TG, sicrhewch eu bod yn gwneud hynny yn ddigonol. Gellir eich dal yn gyfrifol os bydd data personol a gasglwyd gennych yn cael ei echdynnu o'ch hen offer TG wrth ei ailwerthu.



Ble gallaf gael rhagor o wybodaeth?

Beth yw'r broblem?

Fel y nodwyd yn yr ystod o bynciau a drafodwyd yn y canllaw hwn, gall gadw rhwydwaith TG yn ddiogel fod yn dasg gymhleth ac mae'n galw am amser, adnoddau a gwybodaeth arbenigol. Fodd bynnag, mae yna amrywiaeth o sefydliadau yn cynnig cyngor a chanllaw priodol i'ch busnes.

Beth allaf i wneud?

Mae'n anodd darparu ateb syml gan fod pob sefydliad yn prosesu data personol yn wahanol ac mae dan beryg o fygythiadau gwahanol. Fodd bynnag, mae yna nifer o sefydliadau sy'n darparu cyngor yn benodol ar gyfer busnesau bychain.

Dylech annog ymwybyddiaeth gyffredinol o ddiogelwch yn eich sefydliad. Mae diwylliant sy'n ymwybodol o ddiogelwch yn debygol o adnabod risgiau diogelwch. Mae'r ICO yn darparu ystod o adnoddau y gallwch eu harchebu o'r wefan, www.ico.org.uk

Get Safe Online (www.getsafeonline.org)

Menter ar y cyd rhwng y llywodraeth, gwasanaethau gorfodi'r gyfraith, busnesau blaenllaw a'r sector cyhoeddus i ddarparu defnyddwyr cyfrifiaduron a busnesau bychain â chyngor annibynnol a hwylus am ddim a fydd yn eu galluogi i ddefnyddio'r rhyngrwyd mewn modd hyderus a diogel.

Business Link (www.businesslink.gov.uk)

Business Link yw adnodd ar-lein y llywodraeth ar gyfer busnesau. Mae'r safle yn cynnwys gwybodaeth yn ymwneud â diogelwch TG ac e-fasnach ac mae wedi ei dargedu'n benodol at fusnesau.

Mae nifer o werthwyr diogelwch hefyd yn cynnig seminarau, gweminarau, cylchlythyrau, blogiau a chyngor ar eu gwefannau yn ogystal â chynnig archwiliadau diogelwch ffurfiol a gwasanaethau profi diogelwch.

Action Fraud (www.actionfraud.police.uk)

Os ydych chi wedi cael eich twyllo, gallwch roi gwybod i 'Action Fraud' - canolfan hysbysu twyll y Deyrnas Unedig. Gallwch hysbysu 'Action Fraud' am unrhyw dwyll os ydych chi yn y DU, os digwyddodd y twyll yn y DU neu os ydy'r twyll yn gysylltiedig â'r DU ac wedi digwydd ar-lein.

Os hoffech gysylltu â ni, ffoniwch 0303 123 1113

www.ico.org.uk

Swyddfa'r Comisiynydd Gwybodaeth,
Wycliffe House, Water Lane,
Wilmslow, Swydd Gaer, SK9 5AF

Ebrill 2012



Cynnal hawliau gwybodaeth